The International Conference on Information Technology, Coding and Computing, April 2- April 4, 2001, The Orleans' Hotel & Casino, Las Vegas, Nevada, USA; SESSION 3B Recent advances in wireless communications

# Wireless Network Security for Users

Steve F. Russell
*Iowa State University*
*sfr@iastate.edu*

## Abstract

*Network security technology generally concentrates on protection of the network infrastructure and, by implication, the protection of the user. While this is true for the larger public network, the local network environment of the user is very vulnerable to denial-of-service, "man-in-the-middle," and other attacks that can be devastating. In this paper, we examine the issues of wireless security from the perspective of the user and the local network. We will look at airlink attacks by specialized transmitters and intercept receivers. Examples will be taken from the technologies used in IS-95 CDMA cellular radiotelephone and IEEE 802.11 wireless LANs.*

## 1. Introduction

What do wireless users want? In the broadest sense, they want a wireless connection that offers them the same security features as a well-designed and secure wired system. However, even the wired system at the network edge does not provide the security level that will be needed in the future. For wired systems, one need look no further than the fact that after many years, some ethernets and servers still communicate username and password "in the clear" as plain ASCII text [1].

The wireless user will need and want good communication security as they become more reliant on the vast array of digital communication services that are now available or will become available. As they adopt wireless products and communication "habits", they need absolute assurance that their private transactions will be available, accurate, and confidential. Email, mobile phone, and financial transactions come to mind as examples of these private transactions.

Security issues in this paper are addressed primarily to the network edge or local network and wireless access point. In general it is much easier to design and implement good security features inside the larger network hierarchy.

Good communications security and user security features for new products lag far behind the sophisticated technologies that are increasing data bandwidths, improving service, and lowering costs. Effective wireless network security is essential to the future of wireless telecommunications but will be difficult to achieve. Currently, security implementations are somewhat fragmented and lack robustness. There are many reasons for this but first and foremost is that the design and implementation of good security methods will require cooperation among several entities: 1) government regulator, 2) network infrastructure provider, 3) wireless service provider, 4) wireless equipment provider, and 5) wireless user.

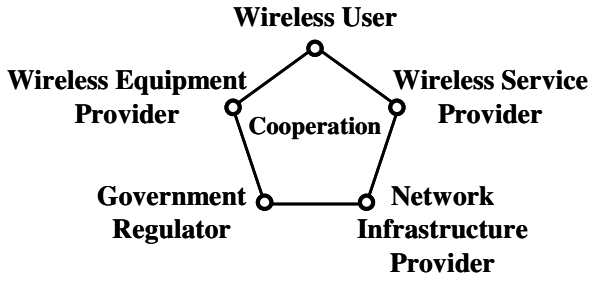


**Figure 1. Cooperation needed among network system entities for good communication system security.**

This cooperation, represented by Fig. 1., has not been achieved to date because of the complicated and competing mix of technologies currently in use. The user has typically been bombarded with marketing literature that touts high data capacity and ease of use but is lacking or even misleading in its claims for security features. Also, because the typical user does not clearly understand the details and implications of security technology, there has been a lack of business and regulatory incentive for improving security. The business relationship among network infrastructure provider, wireless service provider, and wireless equipment provider also inhibits the implementation of comprehensive security measures because it is not easy to share the profits derived from providing good security. A lack of comprehensive security standards also complicates the problem.

Another reason security is lagging far behind technology advances is that the design and implementation of good security methods is costly in terms of processor utilization,

circuit and software design, and data capacity. As scientists, engineers, and technologists, we are loathe to sacrifice good performance in other areas for good security performance that may or may not be a tangible commodity to the user. However, the user is relying on us to provide good security.

In a recent security workshop [2] attended by high-level government policy makers, university researchers, and industry, good discussions were forthcoming on needed government security policy and needed improvements in network security but coverage of issues directly involving civil users were minimal. Again, it is a natural consequence of the roll users play in the overall telecommunication structure and similar to the lack of voice consumers have in product safety decisions.

Finally, there is the issue of the damage, cost, and consequences of a security breech. For example, it is clear that denial-of-service attacks against major Internet companies or against high-level network management and switching systems have a major cost impact for the public in general. However, for the individual user, a security breech can have disastrous individual consequences without affecting the general public or, for that matter, the service and equipment providers - unless litigation is brought by the user. Therefore, how do we justify the need to provide cost-effective and quality wireless network security to the user? This is a question remaining to be answered.

We will now look in more detail at what users need, a description of wireless network security, common wireless security issues, anti-interference technologies for wireless, and solutions needed for better wireless security.

## 2. What do wireless users need?

Wireless users need a wireless airlink that has good availability, range, connectivity, privacy, airlink encryption, and interference immunity, as well as signaling waveforms that cannot easily be intercepted and demodulated. They need all of the traditional security available in a full-featured wired network: access control, anonymity, authentication, availability, certification, information confidentiality, identity confidentiality, encryption, integrity, nonrepudiation, and secrecy. Furthermore, they need status information about the wireless link which would include (as a minimum); airlink connection(s), connection status (ad-hoc mode or infrastructure mode) [3], data rate, quality of signal, noise level, logical wireless channel, and security status summary. In addition, they want control of their wireless terminal in terms of the access levels it permits and the type of information it provides.

Concerning the information provided by a wireless terminal, an example of a major intrusion on privacy is the implementation of FCC mandated E911 for cellular radiotelephone [4]. As initially envisioned, this system could determine the location of every cellular phone within an accuracy of 375 feet 67% of the time. Its ultimate accuracy is planned to be within 40 feet 90% of the time. While being able to send emergency services to the location of a mobile E911 call is of great public benefit, the ability of the system to track all users all of the time has serious privacy implications. A simple solution to this issue is to allow the user to enable or disable this capability for their mobile phone or to simply determine the location only during an E911 call.

## 3. What is wireless network security?

Wireless security as we use it here is a much broader term than is the word security used in the “bank vault” sense. It refers to all aspects of the wireless communication system that make it robust and suitable for the user. Information systems security can be divided into four broad areas: 1) information (data) security, 2) computer security, 3) network security, and 4) wireless channel (airlink) security. We refer to a hybrid of wireless channel security and network security as wireless network security. In essence, it is the security of the airlink and the medium access control associated with wireless access points and ad-hoc wireless networks.

Historically, wireless network security has been seen as primarily an infrastructure and loss-of-revenue issue because these have the largest global monetary impact. An example of this was the cloning of cellular radiotelephones in the early days of cellular. Before the deployment of Personal Communication Systems (PCS) and now 3rd generation (3G) systems, voice communications gave a very limited access to the base station and virtually no access to the network at large. Now however, data traffic and data network protocols such as TCP/IP offer significant network access over a radio link that, except for bandwidth, is equivalent to a wired connection. Thus, we see that there are two major aspects of wireless network security -- security for the user and security for the infrastructure.

Wireless network security differs from the general area of computer and network security in that the airlink is involved and it is mostly concerned with the edge of the network. Many textbooks [5-11] now contain one or more chapters on security and a large body of literature exists for computer and network security but there is only scattered literature for wireless security. This will be rapidly changing.

Secure communications has been a major focus of our military for the past fifty or more years and detailed communication theory literature exists to help designers understand the technology and tradeoffs that apply [12-14]. However this level of sophistication has yet to penetrate the civil side of telecommunications because there has not been a need until now.

## 4. Common wireless security issues

In a short paper, it is not possible to make a comprehensive list of security issues so we will mention the most obvious and probable ones: airlink access, unintentional interference, jamming and/or service degradation, interception, user identity, user position location, data decryption, and network traffic analysis.

Certainly the biggest immediate issue facing this area is the interference that will be caused by the diverse offering of wireless devices and services using the same license-free 2.4 GHz ISM band. In addition to wireless access and networking provided by Wi-Fi, Bluetooth, and HomeRF, there are offerings of cordless phones, wireless audio headsets, and other communication and networking products. Microwave ovens also share the ISM band and create a swept-frequency signal that passes through the band as they cycle on and off.

Misleading information about the interference compatibility of these products is still frequently published. In a recent article on Bluetooth [15], the reviewer installed Bluetooth and WECA 802.11 cards in the same PC and experienced no interference problems. If this appears on the surface to be good news, it belies the fact that although a few devices can operate in the same geographic area, as the density of license-free devices increases, the resulting interference levels increase and the systems fail. Users ultimately will realize this but maybe only after making considerable investments in their wireless infrastructure.

The second biggest issue is denial-of-service caused by intentional jamming. Although not legal, there are cheap devices that can be purchased on the Internet that will jam cellphone, cordless phone, and wireless network communications. Also, an RF engineer using $50 worth of readily-available components can build a simple short-range jammer for any of the common microwave frequencies. Detection and prosecution of people using these devices will be very difficult.

A less-likely but potentially more harmful issue is the use of specialized transmitters and receivers to attack a network. The reason why this is not yet significant is that it requires a level of knowledge and financial investment that, so far, only organizations and governments can provide. Also, the financial or political incentives needed to make attacks on individual users are not yet sufficient to warrant the effort. However, as we rely more and more on wireless to handle important data traffic, these incentives will come.

It probably comes as no surprise to the reader to learn that, in preparation for future conflicts, governments around the world are investigating ways to protect their wireless infrastructure (usually cellular radiotelephone) and at the same time attack and bring down the equivalent infrastructure in other countries. This will have a serious impact on civil users who have come to rely on their cellphones for basic communications.

Another major issue in wireless networks is the data throughput. The throughput is already much smaller than can be achieved with wired networks. Even worse, Fig. 2 illustrates that better wireless security can only be obtained at the price of reduced data throughput. In extreme cases, the throughput can be reduced by 50%. This probably comes as a shock to traditional computer network designers who are used to cyclic redundancy checks (CRCs) and go-back-N protocols that can correct errors with throughput reductions of less than 1%.

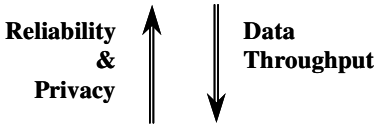


**Fig. 2. Data throughput decreases as reliability and privacy increase.**

The biggest factor causing this difference is that wired networks have extremely small error probabilities whereas wireless networks can have error probabilities orders of magnitude larger. Good adaptive error control methods can make wireless networks much better.

Two general types of attacks can be launched against a wireless network. The first is an attack against the user and the user's airlink. The second is an attack against the network that uses the airlink as a wireless "wiretap." Attacks against the user's airlink are localized and may be harmful only to the user. On the other hand, wireless wiretaps provide access for attacks against the broader network. First we will summarize the attacks against the user's airlink. We will refer to Fig. 3, a summarization of the airlink modeling we use in our work at Iowa State.

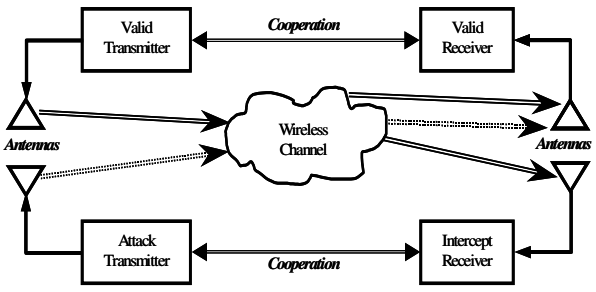


**Figure 3. Wireless channel security scenario.**

The easiest type of attach is denial-of service where the attack transmitter simply transmits on frequencies being used by the valid receiver and transmitter thus blocking communication between the two. A more sophisticated attack would be to intermittently interfere with the system so as to reduce its effectiveness but not trigger its intrusion detection mechanisms.

Another attach we have looked at is the "man-in-the-

middle" where the attack transmitter and receiver cooperate in interception of communications between valid transmitter and receiver. The example we looked at was IS-95 CDMA which does not employ two way authentication. Here the attack transmitter and receiver form a counterfeit (bogus) base station which entices a mobile station requesting call setup to initiate the call with the bogus base. Once the protocols have been exchanged, the bogus base establishes call setup with the authentic base and masquerades as the authentic mobile. Thus, the bogus base is an authentic base to the authentic mobile and an authentic mobile to the authentic base. Once the relay connection is fully established, the bogus base can eavesdrop on the full two-way communication.

In the case of wireless network access, if the attack station can establish false identity with the network, other attacks are possible. If, for example, the attack station can establish itself as a routing node, it can intercept network traffic. It can also violate network rules and degrade network performance.

There are many other possibilities that are too detailed to cover in this paper. One example is "Liberty Crack" as reported in a recent issue of Computer [16]. This Trojan horse program targets handheld devices. Other issues that apply to cellphones are discussed in an article that appeared in the Journal of Electronic Defense [17].

## 5. Practical Anti-interference technologies

Although there are many anti-interference technologies, the most practical for civil telecommunication systems are interference rejection filters, direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), and multi-carrier spread spectrum (MCSS). The most recent technology referred to as ultra-wideband is not a suitable candidate until it can prove itself in a practical radio frequency (RF) environment.

To combat interference, it is not enough to simply say that "spread spectrum" is used and therefore interference is not an issue. The type of spreading used, the system design, and the available RF bandwidths all greatly influence the quality of interference rejection. For example, the type of spreading that can be used in the 2.4 GHz Industrial, Scientific, and Medical (ISM) license-free band [18] has very minimal anti-interference capability unless extremely low (an unacceptable) data rates are used.

### 5.1. Direct-sequence spread spectrum

This method had been around for at least three decades but did not become popular until it was proven effective in the NAVSTAR Global Positioning System (GPS) implemented in the 1980s and 1990s. Its most common civil embodiments are as the cellular radiotelephone standard IS-95 code-division multiple access (CDMA) pioneered by QUALCOMM and as the wireless network access implemented by the Wireless Ethernet Compatibility Alliance (WECA) or "Wi-Fi" group using the IEEE 802.11 standard and the 2.4 GHz ISM license-free band. Essentially, DSSS adds very-high-speed binary phase shift keyed modulation to an RF carrier that is already modulated at a lower-speed data rate. A figure-of-merit for interference rejection in a DSSS system is the processing gain determined as the ratio of the RF bandwidth after spreading to the bandwidth before spreading.

The ability of DSSS to reject unintentional interference and intentional jamming is predicated on having large jamming margins and very long pseudorandom code sequences. If either of these conditions are not met, the DSSS ability to reject interference is seriously compromised. For example, in the GPS, the signaling rate is 50 baud, the chipping rate 10 megachips-per-second, and the code sequence is 604,800 seconds long. Since the Fourier period for the periodic code sequence is the length of the code sequence, the separation of Fourier frequency components is the inverse of the period or 1.65 microhertz! This extremely narrow separation greatly exceeds the criterion for long sequences and a valid processing gain for GPS can be calculated at 200,000.

In contrast, the DSSS implementation of the IEEE 802.11 standard by the WECA group has processing gains of 11 or less. Such small processing gains offer only very modest interference rejection and are easily overwhelmed by the near-far aspect of both intentional and unintentional interference. In IS-95 CDMA cellular radiotelephone, DSSS is used primarily for multiple access and multipath and not as an interference reduction method.

It's the nature of DSSS signals that a small portion of the RF spectrum can be "notched out" and still maintain good performance. This means that DSSS performance for narrowband interference can be greatly improved by using adaptive narrowband reject filters.

### 5.2. Frequency-hopping spread spectrum

The ability of FHSS to reject interference is predicated on having a large number of non-overlapping hopping channels and interleaving of the data so that the system can withstand bursts of interference or noise. The processing gain is simply equal to the number of non-overlapping hopping channels. In the case of the 2.4 GHz ISM band, the processing gain can be 79, which is better than 2.4 GHz DSSS but still very modest.

Interleaving is essential for good interference rejection in FHSS but long hopping dwell times ( up to 400 milliseconds as allowed by the FCC regulations) will produce unacceptably long data latency. The latency produced by a Bluetooth dwell time of 625 microseconds is much more acceptable.

FHSS works reasonably well when the interference or noise is unintentional but can be seriously compromised when a follower jammer is used. To avoid this, it is important to use a large number of hops per second. FHSS does not use a narrowband rejection filter since the receivers already divide the signal into narrow bands. The exception would be to provide a rejection filter to reduce front-end overload in the receiver.

Bluetooth implements FHSS and Home RF is a consortium of companies that have implemented FHSS using the 2.4 GHz ISM band and the IEEE 802.11 specification.

### 5.3. Multi-carrier spread spectrum

Originally conceived as a method of combating multipath interference, multi-carrier spread spectrum (MCSS) also has the capability to reject most types of narrowband interference. As an interference rejection method, its properties are a mix of the properties of DSSS and FHSS. It essentially uses the narrowband carrier of FHSS but combines many of them to fill an RF spectrum as broad as the bandwidth of DSSS. It naturally introduces data interleaving by virtue of the modulation scheme but does not introduce the latency problems attendant to interleaved FHSS. A narrowband rejection filter is not effective help for MCSS because it removes the desired narrowband carrier along with the unwanted narrowband interference.

### 5.4. Narrowband rejection filters

Frequency adaptive, narrowband reject filters used at the front of a receiver can be very effective in reducing the noise and front-end overload caused by a strong narrowband interferer. It can be used in any type of receiver to reduce overload but its best application is in DSSS systems where it can remove the interferer before the despreading correlator. This can greatly reduce the broadband noise after the correlator.

### 5.5. Interference avoidance

With this method, the wireless system monitors the interference spectra within the band of available RF channels and selects the channel that has the lowest level of interference noise. If that channel becomes noisy, the system changes the RF channel to one with lower noise. This method is most effective against unintentional interferers and least effective against intelligent jammers.

## 6. Solutions for better wireless network security

Currently, good design and development cooperation between the wireless equipment provider and network infrastructure provider has the best chance of providing good security features to the user. Government regulations may impose restrictions but good improvement can still be made.

Good security should be an added feature in existing wireless communication devices. Users that don't need or want it should not have to pay for it. On the other hand, users that want very secure communication devices should have that option available to them at an acceptable cost. For example, users could be offered the use of compatible but specialized user equipment when better security is needed. This is already being done in some cellular systems for large-scale emergency communications [19] where public safety officials are issued special cellphones that have good interference immunity and priority access to the cell tower.

The best security will be achieved when security features are added at each networking layer and each physical entity of the network. It is not enough to simply encrypt the source data or provide simple spread spectrum at the physical layer. However, well-designed spread-spectrum should be an essential feature of new designs.

Wireless airlinks must employ highly adaptive error detection and correction algorithms if the raw data throughput is to be efficiently preserved. This means that the algorithm must recognize the basic error rate of the airlink and adjust its robustness and efficiency accordingly. For example, a simple CRC code may be used when errors are very low while a long Reed-Solomon code with interleaving may be used when the errors are high.

Intrusion detection is essential. Zhang and Lee [20] have outlined the intrusion issues for wireless ad-hoc networks and conclude that an intrusion detection agent (IDS) for all nodes is a key architecture. They also point out that detection must be both node-local and node-cooperative in that collective statistics can be gathered so the network as a whole can make a decision about intrusion. It is best to avoid ad-hoc networks except where its benefits outweigh the security risks.

A robust medium access control (MAC) designed for mobility and security is another essential need for wireless. There is currently considerable research and development on wireless MAC and we should expect good solutions in the next year or two. The MAC and physical layer designs should have error detection and correction algorithms that adapt to different airlink error rates. They should have smaller data packets, robust ACK/NAK for uncorrectable errors, and use data interleaving to mitigate unsophisticated jammers. At some rather high level of errors, the data channel will still function but voice over data will probably be impractical.

Higher quality RF designs are needed for mobile units. Base units should consider the use of smart antennas to reduce interference. All receivers should have good anti-

jam design, be protected against front-end overload by good preselector filters, and when necessary, have narrowband reject filters.

Frequency hopping is a superior anti-interference design when its data latency can be tolerated.

All systems should have two-way authentication and user equipment should allow several levels of user intervention to protect against intrusion. At a minimum, the user should be able to ask for re-authentication of the access point or an entire ad-hoc network if needed.

Newer, somewhat novel ideas such as IP hopping should be considered and field tested for a wireless mobile environment and interference avoidance capability is always a good alternative.

## 7. References


[1] C. Gao, "Security Issues in Wired and Wireless Networks", CprE 537X Project Report, Iowa State University, Ames, Iowa, 2000.

[2] Telecommunications and Information Security Workshop, September 27-29, University of Tulsa, Tusla, OK, 2000.

[3] 3Com, "IEEE 802.11b Wireless LANs", *3Com Corporation website*, Santa Clara, CA, 2000.

[4] B. Kidwell, "Wireless Enhanced 9-1-1, Lucent Technologies", *NCF-97*, Chicago, IL, 1997.

[5] W. Stallings, *Cryptography and Network Security Principles and Practice*, 2nd Ed., Prentice-Hall, Upper Saddle River, New Jersey, 1999.

[6] W. Stallings, *Data and Computer Communications*, 6th Ed., Prentice-Hall, Upper Saddle River, New Jersey, 2000.

[7] L. L. Peterson and B. S. Davie, *Computer Networks: A Systems Approach*, 2nd Ed., Academic Press, New York, 2000.

[8] J. Schiller, *Mobile Communications*, Addison-Wesley, New York, 2000.

[9] M. Y. Rhee, *CDMA Cellular Mobile Communications and Network Security*, Prentice-Hall, Upper Saddle River, New Jersey, 1998.

[10] V. K. Garg, K. Smolik, and J. E. Wilkes, *Applications of CDMA in Wireless / Personal Communications*, Prentice Hall PTR, Upper Saddle River, NJ, 1997.

[11] C. P. Pfleeger, *Security in Computing*, 2nd Ed., Prentice-Hall, Upper Saddle River, New Jersey, 1997.

[12] S. F. Russell and B. Wilkerson, "Anti-jam Techniques for Communication and Navigation Systems", *Rockwell International, Collins Avionics & Missiles Group*, Advanced Technology and Engineering, 1979.

[13]R. L. Peterson, R. E. Ziemer, and D. E. Borth, *Introduction to Spread Spectrum Communications*, Prentice-Hall, Englewood Cliffs, NJ, 1995.

[14] R. A. Dillard and G. M. Dillard, *Detectability of Spread-Spectrum Signals*, Artech House, Norwood, MA, 1989.

[15] L. Freed, "The First Bluetooth," *PC Magazine*, p 38, Jan 2, 2001.

[16] N. Leavitt, "Malicious Code Moves to Mobile Devices", *Computer*, pp 16-19, December 2000.

[17] K. Kocks, "Who is afraid of wireless phones", *Journal of Electronic Defense*, April, 1999.

[18] Federal Communications Commission, "Operation within the bands 902-928 MHz, 2400-2483.5 MHz, and 5725-5850 MHz", *Code of Federal Regulations*, Title 47, Volume 1, Part 15, Section 15.247, Rev: Oct. 1, 1999

[19] G. Oster, *Private communication*, Iowa State University Fire Institute, Ames, Iowa, 2001.

[20] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", *Proceedings of the sixth annual International Conference on Mobile computing and Networking (MobiCom 2000)*, Boston, Massachussetts, Aug 6-11, 2000.